CLAIMS

What is claimed is:

1. A trusted execution environment construction method, wherein the method comprises the following:

obtaining regulatory requirement information of a trusted execution environment;

parsing the regulatory requirement information to obtain atomized security function information that is applied to the trusted execution environment;

performing formal parsing processing on the security function information to obtain a security solution of the trusted execution environment, wherein the security solution can prove that it satisfies the regulatory requirement information, and generating a test case corresponding to the security solution of the trusted execution environment based on an axiom of the security solution of the trusted execution environment; and

constructing, by using a predetermined property migration mechanism based on the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, a trusted execution environment that has same property information as the security solution and the test case with respect to a predetermined property item in a target scenario,

wherein the property migration mechanism is a processing mechanism for migrating a property of an object that has been verified or authenticated to another object having a specified association relationship with the object,

wherein the predetermined property item comprises one or more property items, and

wherein the property information is content information corresponding to the predetermined property item.

2. The method according to claim 1, wherein the constructing, by using a predetermined property migration mechanism based on the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, a trusted execution environment that has same property information as the security solution and the test case with respect to a predetermined property item in a target scenario comprises the following:

constructing a security sub-solution of the trusted execution environment in the target scenario by using a homomorphism interpretation based on the security solution of the trusted execution environment;

obtaining constraint information of the trusted execution environment in the target scenario; and constructing a test sub-case of the trusted execution environment in the target scenario by using a homomorphism interpretation with reference to the constraint information based on the test case corresponding to the security solution of the trusted execution environment; and

generating the trusted execution environment in the target scenario by using modified condition and decision coverage (MC/DC coverage) based on the test sub-case of the trusted execution environment in the target scenario.

3. The method according to claim 2, wherein the target scenario comprises one or more of an Internet of Things scenario, a cloud scenario, and a terminal device scenario.

4. The method according to claim 3, wherein the target scenario comprises multiple different scenarios, and a property of the security sub-solution of the trusted execution environment is migrated between security sub-solutions of the trusted execution environment in different scenarios by a natural transformation.

5. The method according to claim 3, wherein the target scenario comprises multiple different scenarios, and a property of the test sub-case of the trusted execution environment is migrated between test sub-cases of the trusted execution environment in different scenarios by a natural transformation.

6. The method according to claim 1, wherein the parsing the regulatory requirement information to obtain atomized security function information that is applied to the trusted execution environment comprises the following:

obtaining security function information constituting the security solution; and

performing disassembly processing on the regulatory requirement information by using information security common criteria (CC) based on the obtained security function information constituting the security solution, so as to obtain the atomized security function information that is applied to the trusted execution environment.

7. The method according to claim 6, wherein a mutually exclusive collectively exhaustive (MECE) rule is satisfied between different security functions in security functions corresponding to the atomized security function information.

8. The method according to claim 1, wherein the performing formal parsing processing on the security function information to obtain a security solution of the

trusted execution environment, wherein the security solution can prove that it satisfies the regulatory requirement information comprises the following:

performing formal parsing processing on the security function information to obtain a preselected security solution of the trusted execution environment;

performing, based on the preselected security solution of the trusted execution environment and the regulatory requirement information of the trusted execution environment, processing of verification on whether the preselected security solution of the trusted execution environment satisfies the regulatory requirement information of the trusted execution environment, so as to obtain a corresponding verification result; and

if the verification result indicates that the preselected security solution satisfies the regulatory requirement information of the trusted execution environment, using the preselected security solution as the security solution of the trusted execution environment.

9. The method according to any one of claims 1 to 8, wherein the trusted execution environment comprises one or more of a trusted execution environment constructed by using SGX and a predetermined first application program, a trusted execution environment constructed by using TrustZone and a predetermined second application program, and a trusted execution environment constructed by using a predetermined third application program.

10. A trusted execution environment construction apparatus, wherein the apparatus comprises the following:

a regulatory requirement acquisition module, configured to obtain regulatory requirement information of a trusted execution environment;

a regulatory requirement parsing module, configured to parse the regulatory requirement information to obtain atomized security function information that is applied to the trusted execution environment;

a processing module, configured to perform formal parsing processing on the security function information to obtain a security solution of the trusted execution environment, wherein the security solution can prove that it satisfies the regulatory requirement information, and generate a test case corresponding to the security solution of the trusted execution environment based on an axiom of the security solution of the trusted execution environment; and

a trusted environment construction module, configured to construct, by using a predetermined property migration mechanism based on the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, a trusted execution environment that has same property information as the security solution and the test case with respect to a predetermined property item in a target scenario,

wherein the property migration mechanism is a processing mechanism for migrating a property of an object that has been verified or authenticated to another object having a specified association relationship with the object,

wherein the predetermined property item comprises one or more property items, and

wherein the property information is content information corresponding to the predetermined property item.

11. The apparatus according to claim 10, wherein the trusted environment construction module comprises the following:

a sub-solution construction unit, configured to construct a security sub-solution of the trusted execution environment in the target scenario by using a homomorphism interpretation based on the security solution of the trusted execution environment;

a sub-case construction unit, configured to obtain constraint information of the trusted execution environment in the target scenario; and construct a test sub-case of the trusted execution environment in the target scenario by using a homomorphism interpretation with reference to the constraint information based on the test case corresponding to the security solution of the trusted execution environment; and

a trusted-environment construction unit, configured to generate the trusted execution environment in the target scenario by using modified condition and decision coverage (MC/DC coverage) based on the test sub-case of the trusted execution environment in the target scenario.

12. The apparatus according to claim 11, wherein the target scenario comprises multiple different scenarios, and a property of the security sub-solution of the trusted execution environment is migrated between security sub-solutions of the trusted execution environment in different scenarios by a natural transformation.

13. The apparatus according to claim 11, wherein the target scenario comprises multiple different scenarios, and a property of the test sub-case of the trusted execution

environment is migrated between test sub-cases of the trusted execution environment in different scenarios by a natural transformation.

14. A trusted execution environment construction device, comprising:

a processor; and

a storage configured to store a computer-executable instruction, wherein when the executable instruction is executed, the processor is enabled to:

obtain regulatory requirement information of a trusted execution environment;

parse the regulatory requirement information to obtain atomized security function information that is applied to the trusted execution environment;

perform formal parsing processing on the security function information to obtain a security solution of the trusted execution environment, wherein the security solution can prove that it satisfies the regulatory requirement information, and generate a test case corresponding to the security solution of the trusted execution environment based on an axiom of the security solution of the trusted execution environment; and

construct, by using a predetermined property migration mechanism based on the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, a trusted execution environment that has same property information as the security solution and the test case with respect to a predetermined property item in a target scenario,

wherein the property migration mechanism is a processing mechanism for migrating a property of an object that has been verified or authenticated to another object having a specified association relationship with the object,

wherein the predetermined property item comprises one or more property items, and

wherein the property information is content information corresponding to the predetermined property item.

15. A storage medium, wherein the storage medium is configured to store a computer-executable instruction, and the executable instruction is executed to implement the following procedure:

obtaining regulatory requirement information of a trusted execution environment;

parsing the regulatory requirement information to obtain atomized security function information that is applied to the trusted execution environment;

performing formal parsing processing on the security function information to obtain a security solution of the trusted execution environment, wherein the security

solution can prove that it satisfies the regulatory requirement information, and generating a test case corresponding to the security solution of the trusted execution environment based on an axiom of the security solution of the trusted execution environment; and

constructing, by using a predetermined property migration mechanism based on the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, a trusted execution environment that has same property information as the security solution and the test case with respect to a predetermined property item in a target scenario,

wherein the property migration mechanism is a processing mechanism for migrating a property of an object that has been verified or authenticated to another object having a specified association relationship with the object,

wherein the predetermined property item comprises one or more property items, and

wherein the property information is content information corresponding to the predetermined property item.